UMBRELLA DATA SHARING AGREEMENT K__3723____
BETWEEN
STATE OF WASHINGTON
OFFICE OF FINANCIAL MANAGEMENT
AND

AGENCY NAME Criminal Justice Training Commission **DSA #** IA22-020

Table of Contents

UMBRELLA DATA SHARING AGREEMENT

This Umbrella Data Sharing Agreement ("DSA or Agreement") is entered into by and between the **OFFICE OF FINANCIAL MANAGEMENT**, hereinafter referred to as "OFM or DATA PROVIDER", and Washington State

Agency Name	Criminal Justice Training Commission

hereinafter referred to as "RECIPIENT", pursuant to the authority granted by chapter 39.34 of the Revised Code of Washington, relevant federal statutes, and related regulations.

OFM DSA Administrator:		**RECIPIENT** DSA Administrator	
Name:	Becci Riley	Name:	Brian Elliott
Title:	Executive IT Contracts Administrator	Title:	Financial Manager
Division:	Legal & Legislative Affairs	Division:	Fiscal
Address:	302 Sid Snyder Ave SW Olympia, WA 98501	Address:	3060 Willamette Dr. Lacey, WA 98516
Phone:	360.522.3575	Phone:	360-281-9346
E-mail:	Becci.riley@ofm.wa.gov	E-mail:	belliott@cjtc.wa.gov

1. **UMBRELLA DSA APPLICABILITY**

    This Umbrella DSA applies to all Data shared between the parties and documents the general terms and conditions, procedures, roles and responsibilities, and appropriate data security constraints required for the accurate exchange of Data between the parties.

    Data Sharing Addendum (Addendum): Specific Data provided to RECIPIENT will be documented in addenda that will document the purpose for which the Data is shared. Each Addendum will be attached and subject to this DSA. Each Addendum will include any additional or special requirements for handling of the Data that is the subject of the Addendum.

2. **DEFINITIONS**

    "Addendum" means an attachment to this Data Sharing Agreement that describes the Data or information to be shared with RECIPIENT and the handling of such Data, which may be in addition to the requirements in the body of this Agreement or specific to the activities authorized under the addendum.

    "Agreement" means this Data Sharing Agreement, including all documents attached or incorporated by reference.

    "Data Access" refers to methods and rights granted to RECIPIENT to receive Data.

    "Data Classification" refers to the sensitivity of Data as defined by the Office of the Chief Information Officer (OCIO) in OCIO Standard 141.10, as may be modified by the OCIO from time to time. Current categories are set forth in Attachment 1, OCIO Data Classification.

    "Data Encryption" refers to ciphers, algorithms or other encoding mechanisms that will encode Data to protect its confidentiality. Data encryption may be required during data transmission and/or data storage depending on the level of protection required for this Data.

    "Data Storage" refers to the state Data is in when at rest.

    "Data Transmission" refers to the methods and technologies to be used to move a copy of the Data between systems, networks, and/or workstations.

    "Disclosure" means to permit access to or release, transfer, or other communication of Data or information by any means including oral, written, or electronic means.

"Data" means information, including but not limited to PII, provided by OFM under this DSA, whether that information originated in OFM or in another entity.

"OCIO" means the Washington State Office of the Chief Information Officer.

"Personally Identifiable Information (PII)" means information identifiable to any person, including, but not limited to, information that relates to a person's name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, social security numbers, driver's license numbers, credit card numbers, any other identifying numbers, and any financial identifiers.

3. PERIOD OF AGREEMENT

This DSA shall begin on the date of execution and end on June 30, 2026 unless terminated sooner or extended as provided herein. This DSA may be extended as needed by the parties in up to three (3) year increments. Such extensions will be by mutual agreement and will be in the form of written amendment(s) to this DSA.

The parties agree that they will review the terms and conditions of this DSA and any then current Addendum at least annually to ensure that the content is accurate.

The term of any Addendum executed under this DSA will be stated therein. The expiration date of any Addendum may not exceed the then-current expiration date of this DSA.

4. DATA SECURITY (OCIO 141.10.4.2(5)); (OCIO 141.10.4.2(6))

Any data-specific requirements related to the subjects in this section will be set out in addenda to this DSA.

a. Authorized Access Only
Access to the Data provided by OFM will be restricted to RECIPIENT staff, officials, and agents who are authorized to access the Data and need it to perform their official duties as detailed in the Addendum under which the Data is shared.

b. Data Storage
All Data provided by OFM must be stored in a secure environment with access limited to the least number of RECIPIENT staff, officials, and agents needed to complete the purpose of the Addendum under which the Data is shared.

c. Data Protection
In all cases and under each Addendum, RECIPIENT will take due care and take reasonable precautions to protect OFM provided Data from unauthorized physical and electronic access. RECIPIENT will strive to meet or exceed the requirements of the OCIO policies and standards outlined in policy 141.10 (located at: https://ocio.wa.gov/policy/securing-information-technology-assets-standards) for data security and access controls to ensure the confidentiality, availability and integrity of all Data shared.

d. IT Data Security Administration
RECIPIENT's IT Data Security Administrators will provide to the OFM IT Data Security Administrator relevant documentation that outlines the data security program components supporting data shared under each Addendum. This documentation will define all data security methods and technology for each individual data exchange to ensure RECIPIENT is in compliance with all appropriate OCIO security standards and/or other applicable standards for such data.

This documentation will serve to satisfy any potential requirement each agency may have under OCIO Security Standards to document the management and security of Data and information.

5. **DATA CONFIDENTIALITY**

RECIPIENT acknowledges the personal or confidential nature of the Data shared hereunder and agrees that RECIPIENT staff with access to the Data will comply with all laws, regulations, and policies that apply to protection of the confidentiality of the Data. If Data provided under this DSA is to be shared with a contractor, the contract(s) must include all of the data security provisions within this DSA and within any amendments, addenda, attachments, or exhibits within this DSA.

a. **Non-Disclosure of Data**
1) Individuals accessing Data by reason of this DSA and its addenda will do so only for the specific purpose described in the Addendum under which the Data is shared. Data may not be repurposed across addenda for any reason.

2) OFM, at its discretion, may at any time disqualify any person from authorized access to Data provided pursuant to this DSA. Notice of disqualification shall be in writing and shall immediately upon delivery of notice to RECIPIENT, terminate the disqualified person's access to any Data provided under this DSA. Disqualification of one or more persons by OFM does not affect other persons authorized by or pursuant to this DSA.

b. **Penalties for Unauthorized Disclosure of Information**
In the event RECIPIENT fails to comply with any term of this DSA, OFM shall have the right to take such action as it deems appropriate to protect the OFM Data from disclosure or otherwise mitigate potential harm resulting from such failure to comply. The exercise of remedies pursuant to this paragraph shall be in addition to all sanctions provided by law, and to legal remedies available to parties injured by unauthorized disclosure.

c. **Data Segregation**
1) OFM Data shall be segregated or otherwise distinguishable from non-OFM Data. This is to ensure that when no longer needed by the RECIPIENT, all OFM Data can be identified for return or destruction. It also aids in determining whether OFM Data has or may have been compromised in the event of a security breach.

2) When it is not feasible or practical to segregate OFM Data from non-OFM Data, then both the OFM Data and the non-OFM Data with which it is commingled shall be protected as described in this DSA and the relevant Addendum under which such Data is shared.

6. **NOTIFICATION OF DATA BREACH**

If RECIPIENT or its agents detect a compromise or potential compromise in the IT security for Data provided under this DSA, such that PII may have been accessed or disclosed without proper authorization, RECIPIENT must give notice to OFM within one (1) business day of discovering the compromise or potential compromise. RECIPIENT must take corrective action as soon as practicable to eliminate the cause of the breach and, in consultation and collaboration with OFM, shall be responsible for ensuring that appropriate notice is made to those individuals whose personal information may have been improperly accessed or disclosed. In addition, if credit monitoring is required as a result of the breach, then RECIPIENT will be financially responsible for the cost of such credit monitoring.

7. DISPOSITION OF DATA

Upon termination of this DSA, or any Addendum subject to this DSA, RECIPIENT agrees to erase, destroy, and render unreadable all Data received under this DSA or the relevant Addendum and provide written notification (See Exhibit A, Certification of Data Disposition) within fifteen (15) days of the date of disposal to the Addendum Administrators with a copy to the OFM DSA Administrator set forth in this DSA. Destruction methods must comply with OCIO policy 141.10 section 8.3 and follow the OCIO Media Handling and Data Disposal Best Practices. (OCIO 141.10.4.2(7)).

8. ON-SITE OVERSIGHT AND RECORDS MAINTENANCE

RECIPIENT agrees that OFM shall have the right, at any time, to monitor, audit and review activities and methods in implementing this DSA in order to assure compliance therewith, within the limits of RECIPIENT' technical capabilities.

Both parties hereto shall retain all records, books, or documents related to this DSA for six years, except Data destroyed as set forth in the section titled *DISPOSITION OF DATA* of this DSA. The Office of the State Auditor, federal auditors, and any persons duly authorized by the parties shall have full access to and the right to examine any of these materials during this retention period.

9. INDEMNIFICATION

Each party to this DSA shall be responsible for any and all acts and omissions of its own staff, employees, officers, agents and independent contractors. Each party shall furthermore defend and hold harmless the other party from any and all claims, damages, and liability of any kind arising from any act or omission of its own staff, employees, officers, agents, and independent contractors.

10. AMENDMENTS AND ALTERATIONS TO THIS DSA

With mutual consent, OFM and RECIPIENT may amend this DSA at any time, provided that the amendment is in writing and signed by authorized representatives of each party.

11. ORDER OF PRECEDENCE

In the event of an inconsistency in this DSA, an Addendum hereto, or any amendment, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

   a. Applicable Federal and State laws;
   b. The terms and conditions of this DSA whether by reference or otherwise.
   c. Addenda to this DSA

12. TERMINATION

a. <u>For Convenience</u>
Either party may terminate this DSA in whole or in part, including any Addendum attached hereto, with thirty (30) days' written notice to the other party's Agreement Administrator named on Page 1. In case of termination, any and all Data that is the subject of such termination that was provided by OFM pursuant to this DSA shall either be immediately returned to OFM or immediately destroyed, as instructed by OFM. As set forth in the section titled *DISPOSITION OF DATA* of this DSA, written notification to OFM confirming the disposition of the Data must be given.

b. <u>**For Cause**</u>

OFM may terminate this DSA, in whole or in part, at any time prior to the date of completion if and when it is determined that RECIPIENT has failed to comply with the conditions of this DSA. OFM shall promptly notify RECIPIENT in writing of the termination and the reasons for termination, together with the effective date of termination. In case of termination, the Data provided by OFM shall be returned to OFM or destroyed on or before the date of termination, as instructed by OFM. As set forth in the section titled *DISPOSITION OF DATA* of this DSA, written notification to OFM confirming the disposition of the Data must be given.

13. GOVERNING LAW

This DSA, including any amendments, addenda, attachments, or exhibits hereto, shall be construed under the laws of the State of Washington. Venue shall be proper in Superior Court in Thurston County, Washington.

14. SEVERABILITY

The provisions of this DSA are severable. If any provision of this DSA is held invalid by any court; that invalidity shall not affect the other provisions of this DSA and the invalid provision shall be considered modified to conform to the existing law.

15. SIGNATURES

The parties have read and understand this DSA and hereby assert that they are authorized to enter into this DSA on behalf of their organization. The signatures below indicate agreement between the parties.

OFFICE OF FINANCIAL MANAGEMENT

RECIPIENT: Criminal Justice Training Commission

DocuSigned by:

Roselyn Marcus 02/17/2022
30768E7E7E2D4EB...

Signature   Date

Roselyn Marcus
Printed Name
Assistant Director
Legal & Legislative Affairs
Title

DocuSigned by:

Kevin Zeller 02/24/2022
6494F9EB76D0400...

Signature   Date

Kevin Zeller
Printed Name

Assistant Director
Title

APPROVED AS TO FORM:

Cam Comfort, AAG

/s/ 1.31.2022

EXHIBIT A
Certification of Data Disposition

Recipient Agency Name: Criminal Justice Training Commission

OFM Data Sharing Agreement (DSA) Number: __K 3723__

OFM Data Sharing Addendum: Addendum for One Washington Project   Dated: 02/24/2022

Date of Disposition _____

Media (type, serial number, other unique identifiers) _____

Date the media was sanitized: _____

The person performing the activity was: _____

The method used (reference Office of the Chief Information Officer standard 141.10 at https://ocio.wa.gov/policy/media-handling-and-data-disposal-best-practices for most current acceptable methods) to render all Data unusable (e.g. software tool used and/or physical destruction of the media) was:

_____

All copies of any Data sets related to this DSA/Addendum that have not been disposed of in a manner described above, have been returned to OFM's Addendum Administrator named below:

      Name/Title _____

Media to be disposed must stay within the control of the agency from the time it is collected until the time it is sanitized. Storage media to be disposed should be collected by, and in the constant possession of dedicated, trusted personnel. Media must be maintained in a secure, locked area until it can be sanitized.

By the authorized signature below, the Data Recipient hereby certifies that the Data provided by OFM has been handled and rendered unusable as indicated above and as required in the DSA designated above.

Signature of Recipient Addendum Administrator _____ Date: _____

Name/Title _____

Return original to OFM Addendum Administrator indicated on page 1 of the referenced Addendum. Retain a copy for your records.

ATTACHMENT 1
OCIO Data Classification

Office of the Chief Information Officer DATA CLASSIFICATION as set forth in OCIO Standard 141.10

Category 1 – Public Information. Public information that can be or currently is released to the   public. It does not need protection from unauthorized disclosure, but does need integrity and   availability protection controls.

Category 2- Sensitive Information. Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

Category 3 – Confidential Information. Confidential Information is information that is specifically protected from either release or disclosure by law. It may include but is not limited to:

      a.   Personal information as defined in RCW 42.56.590(10) and RCW 19.255.010. Information about public employees as provided in RCW 42.56.250.
      b.   Lists of individuals for commercial purposes as provided in RCW 42.56.070(8).
      c.   Information about the infrastructure and security of computer and telecommunication networks as provided in RCW 42.56.420(4).

Category 4 – Confidential Information Requiring Special Handling. Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

a.   Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements.
b.   Serious Consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

OFFICE OF FINANCIAL MANAGEMENT
DATA SHARING ADDENDUM
FOR
ONE WASHINGTON PROGRAM
SaaS ERP Solution Implementation

TO OFM DSA K 3723	
AGENCY NAME Criminal Justice Training Commission **DSA #** IA22-020	

This Data Sharing Addendum (Addendum) is entered into by and between the OFFICE OF FINANCIAL MANAGEMENT, hereinafter referred to as "OFM or DATA PROVIDER", and Criminal Justice Training Commission _____ hereinafter referred to as "RECIPIENT" and is subject to the terms and conditions of the Umbrella Data Share Agreement (DSA) executed between the parties.

1. PURPOSE OF ADDENDUM

The purpose of this Addendum is to allow Data to be shared between state agencies, agency staff, and contractors who will participate in the implementation of the Workday SaaS ERP Solution (ERP Solution). RECIPIENT is a key participant in the implementation of the ERP Solution. RECIPIENT support and participation is integral to the success of the implementation project. Therefore, RECIPIENT authorized staff and contractors authorized by OFM will have access to information provided and considered to be proprietary and/or confidential. This Addendum documents Data and information that will be shared through the OFM One Washington Program (Program) in the course of the implementation and sets out the Data handling and disposition requirements for such Data and information.

2. TERM

The term of this Addendum will begin on the last date of signature by the parties through June 30, 2026. The Addendum may be extended by the parties as mutually agreed in a written amendment signed by authorized signatories of the parties.

3. ADDENDUM ADMINISTRATION

AGENCY PROVIDING DATA (DATA PROVIDER): OFFICE OF FINANCIAL MANAGEMENT

Addendum Administrator:		Technical Administrator	
Name:	Trish Almond	Name:	Ann Bruner
Title:	Business Operations Manager	Title:	One Washington Chief Technology Officer
Division:	One Washington	Division:	One Washington Program
Address:	128 10th Ave S Olympia, WA 98501	Address:	106 11th Ave SW (106 Building) Olympia, WA 98503
Phone:	360-810-0517	Phone:	360.810.1410
E-mail:	Trish.Almond@ofm.wa.gov	E-mail:	Ann.Bruner@ofm.wa.gov

Security Administrator:	
Name:	John Leahy
Title:	OFM Chief Information Security Officer
Division:	IT Services
Address:	1500 Jefferson Street St. SE, Olympia, WA 98501
Phone:	360/407-2675
E-mail:	John.Leahy@ofm.wa.gov

ORGANIZATION RECEIVING DATA (RECIPIENT): Criminal Justice Training Commission
_____

RECIPIENT Addendum Administrator:		RECIPIENT Technical Administrator	
Name:	Brian Elliott	Name:	Jeff Wilcox
Title:	Financial Manager	Title:	IT Manager
Division:	Fiscal	Division:	Information Technology
Address:	3060 Willamette Dr Lacey, WA 98516	Address:	19010 1st Ave S Burien, WA 98148
Phone:	360-281-9346	Phone:	206-835-7297
E-mail:	belliott@cjtc.wa.gov	E-mail:	jwilcox@cjtc.wa.gov

RECIPIENT Security Administrator:	
Name:	Jeff Wilcox
Title:	IT Manager
Division:	Information Technology
Address:	19010 1st Ave S Burien, WA 98148
Phone:	206-835-7297
E-mail:	jwilcox@cjtc.wa.gov

4. **DESCRIPTION OF DATA TO BE SHARED (OCIO 141.10.4.2(1)) (OCIO 141.10.4.2(3))**

As set forth in the DSA, "Data" is defined by OCIO Security Standard 141.10. The highest level of Data shared hereunder contains:

> **Category 3 – Confidential Information.** Confidential Information is information that is specifically protected from either release or disclosure by law. It may include but is not limited to:
>
> a. Personal information as defined in RCW 42.56.590(10) and RCW 19.255.010. Information about public employees as provided in RCW 42.56.250.
> b. Lists of individuals for commercial purposes as provided in RCW 42.56.070(8).
> c. Information about the infrastructure and security of computer and telecommunication networks as provided in RCW 42.56.420(4).

Office Of Financial Management Data Sharing Addendum
For One Washington Program SaaS ERP Solution Implementation

The Data to be shared hereunder will be:

Due to the statewide transformational nature of the ERP Solution and its implementation, it is expected that participants may be exposed to broad data sets that include, but are not limited to:

>   **AFRS:** financial data about individuals, contractors, banks, etc.
>   **Procuremen**t: data claimed to be confidential or proprietary by third party providers, data about individuals receiving government services, county-level data, legal settlements, etc.
>   **HR/Payrol**l: data related to individual financial circumstances such as payroll deductions, leave balances, etc.
>   **Budge**t: budget development information (work in progress)

Third Party Claimed Confidential Information:

In addition to the state owned Data, OFM/One Washington has contracted with the ERP Solution provider, Workday, and certain other third party contractors for assistance and associated guidance in the implementation of the ERP Solution. Those third party contractors may provide tools, methods, documentation and other data that the contractor considers to be Third-Party Claimed Confidential Information. RECIPIENT will treat such data as confidential for the purposes of its use under this Addendum.

Information provided by OFM contractors may be provided in the following ways: (1) it is or was disclosed in tangible form and is conspicuously marked "Proprietary," "Confidential" or the like or (2) it is or was disclosed in non-tangible form, identified as confidential at the time of disclosure and summarized in tangible form conspicuously marked "Proprietary," "Confidential" or the like within thirty (30) days of the original disclosure.

"Third-Party Claimed Confidential Information" means third-party information provided in the course of the implementation and maintenance of the ERP Solution that is claimed by the third party to be confidential. Such information includes, but is not limited to: (a) any software utilized by such third parties in the provision of the service to the state of Washington and its respective source code; (b) non-public business or technical information, including but not limited to the documentation, training materials, any information relating to software product plans, designs, internal costs, and product names, finances, marketing plans, business opportunities, personnel, research, development or know-how that is designated by the disclosing party as "confidential" or "proprietary" or the receiving party knows or should reasonably know is confidential or proprietary.

5. **INTENDED USE OF DATA**

The Data shared under this Addendum will be used solely for the purpose of implementing the ERP Solution under the direction of the OFM/One Washington Program, according to approved project parameters. **The Data may not be used for any other purpose.**

This Agreement does not constitute a release of the Data for the RECIPIENTs discretionary use, but may be accessed only to carry out the responsibilities in support of the ERP Solution implementation and for the purposes described herein.   Any ad hoc analyses or other use of the Data, not specified in this Addendum, is not permitted without the prior written approval of OFM.

---

6. **DATA ACCESS (OCIO 141.10.4.2(4)); (OCIO 141.10.4.2(5))**

Access to the Data provided by OFM must be restricted to RECIPIENT staff, officials, contractors, and agents of the parties who are authorized to access the Data and need it to perform their official duties as detailed in the Purpose of Addendum section of this Addendum.

RECIPIENT may not share in any manner whether verbally or otherwise, work products in any state of development to any unauthorized person.

Data may be accessed in multiple formats and methods under this Addendum (See DATA TRANSMISSION below). Regardless of the format or delivery method, RECIPIENT is obligated to maintain confidentiality of such Data.

Access is granted only for the purpose set out in this Addendum. All individuals authorized to access OFM Data must comply with the requirements of this Addendum and the DATA CONFIDENTIALITY section of the DSA to which this Addendum is attached.

7. **DATA TRANSMISSION (OCIO 141.10.4.2(4)); (OCIO 141.10.4.4)**

Data may be transmitted in the following ways, including but not limited to:

> Electronically in virtual meetings using tools necessary to support the implementation such as:
> > Microsoft Teams
> > Zoom
> > Skype
> > Other electronic meeting forums as determined by the OFM One WA Program.
> SharePoint
> Basecamp
> Secure File Transfer Protocol (SFTP)
> Tools provided by the Strategic Integrator (SI)
> Use of SI cloud services
> Microsoft Office Suite (Word, Excel, Outlook, etc.)
> Surveys
> Via the State Government Network (SGN)
> Within the Workday ERP Solution as authorized and using designated security protocols
> As otherwise provided, in any form, through the One Washington Program.

8. **DATA SECURITY (OCIO 141.10.4.2(5)); (OCIO 141.10.4.2(6))**

a. **Data Storage**

All Data provided by OFM will be stored in a secure environment with access limited to the least number of staff needed to complete the purpose of this Addendum. RECIPIENT agrees to store Data in the following manner and to protect the Data as described:

---

1) Network server disks. Data will be stored on hard disks mounted on network servers and made available through shared folders. Access to the Data shall be restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. to removable media.

2) RECIPIENT will **not** store any confidential or sensitive OFM Data provided pursuant to this Addendum on any external drives or portable electronic devices or media, including, but not limited to laptops, handhelds/PDAs, Ultra-mobile PCs, flash memory devices, floppy discs, optical discs (CDs/DVDs), portable hard disks, and personal or temporary cloud-based accounts.

3) No agency will have or hold any Data on its own systems.

4) Access to data will be via multi-factor authentication (MFA), u*se of SFTP, Active Directory, or networks that have built-in security, including: the Public Governmental Network (PGN), Secure Governmental Network (SGN), the Inter-gov Network (IGN).*

9. TERM OF CONFIDENTIALITY REQUIREMENTS

Except as otherwise specified herein, the requirement in this Addendum to maintain the confidentiality of Data is perpetual and does not cease with the expiration or termination of this Addendum.

10. AMENDMENTS AND ALTERATIONS TO THIS ADDENDUM

With mutual consent, OFM and RECIPIENT may amend this Addendum at any time provided that the amendment is in writing and signed by authorized representatives of each party.

11. SIGNATURES

The parties have read and understand this One Washington Program Addendum and the DSA to which it is attached. The signatories below hereby assert that they are authorized to enter into this Addendum on behalf of their organization. Therefore, the signatories below indicate agreement between the parties.

OFFICE OF FINANCIAL MANAGEMENT

DocuSigned by:

Roselyn Marcus

30768F7E7F2D4EB...

Signature

Roselyn Marcus

Printed Name

Assistant Director

Legal & Legislative Affairs

Title

02/17/2022

Date

Agency: Criminal Justice Training Commission

DocuSigned by:

Kevin Zeller

6494F9EB76D0400...

Signature

Kevin Zeller

Printed Name

Assistant Director

Title

02/24/2022

Date

Office Of Financial Management Data Sharing Addendum
For One Washington Program SaaS ERP Solution Implementation